Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

REPLY COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD., AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit these reply comments regarding the Second Further Notice of Proposed Rulemaking ("Second FNPRM")[1] in the above-captioned docket.

In implementing the Secure Networks Act,[2] the Commission must abide by the Act's plain text, which curtails the Commission's discretion and confirms that the Commission lacks authority to make national security determinations of its own. Moreover, the Commission must add equipment and services to the Covered List only if that equipment or those services meet specific characteristics prescribed by Section 2(b)(2) of the Secure Networks Act. Finally, the Commission must use a transparent process, providing notice before adding equipment or services to the Covered List in order to ensure that it complies with the requirements of the Act and does not violate

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 20-99 ("Second FNPRM").

[2] *See* Pub. L. 116-124, 133 Stat. 158 (2020) (the "Secure Networks Act").

the due process rights of entities that may not have had prior knowledge or an opportunity to challenge the specific determinations upon which the Commission intends to rely to place equipment on the Covered List.

I. THE PLAIN TEXT OF THE SECURE NETWORKS ACT REQUIRES THE COMMISSION TO RELY EXCLUSIVELY ON OTHER ENTITIES' NATIONAL SECURITY JUDGMENTS.

A. There is broad agreement among commenting parties that the Secure Networks Act, by its terms, requires the Commission to rely exclusively on the national security judgments of other agencies, and of Congress in the National Defense Authorization Act of 2019 ("2019 NDAA"), in identifying equipment and services to include on the Covered List.[3] As NCTA notes, the threshold predicate for Commission authority under the Secure Networks Act is a national security risk determination by a specified executive branch agency or Congress under Section 889 of the 2019 NDAA.[4] Because the Secure Networks Act dictates that the Commission's determination of "'covered equipment or services' must originate solely with Section 2(c) determinations," the Act denies the Commission any role in making national security determinations.[5]

Commenting parties agree that the Secure Networks Act confirms that the Commission has no authority to make national security determinations and therefore necessarily agree that the *Supply Chain Order* has no basis in statute.[6] The Secure Networks Act does not "grant the Commission

---

[3] *See, e.g.*, Comments of Competitive Carriers Association, WC Docket No. 18-89, at 4-5 (filed Aug. 31, 2020) ("CCA Comments") (stating that the Commission should rely on the judgements of national security agencies in developing the Covered List).

[4] *See* Comments of NCTA – The Internet & Television Association, WC Docket No. 18-89, at 5 (filed Aug. 31, 2020) ("NCTA Comments").

[5] Comments of USTelecom – The Broadband Association, WC Docket No. 18-89, at 3 (filed Aug. 31, 2020) ("USTelecom Comments").

[6] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423

plenary authority to regulate the communications network supply chain based upon its own assessment of national security risks posed by covered equipment and services."[7] Rather, "because the Commission's determination of 'covered equipment or services' must originate 'solely' with section 2(c) determinations, the statute eliminates the Commission's discretion to determine the equipment that poses a threat to national security on its own."[8] In short, commenters agree that the Commission must follow the text of the Secure Networks Act in preparing the Covered List by relying exclusively on "specific [national security] determination[s]" made either by Congress in the 2019 NDAA or by other, specifically enumerated agencies with national security expertise.

B. Huawei agrees with other commenters that relying on determinations by the Committee on Foreign Investment in the United States ("CFIUS") or Team Telecom—neither of which is mentioned in the Secure Networks Act—would reduce predictability and stability.[9] CFIUS determinations are made through a highly confidential process. Except in rare cases in which a transaction has been referred to the President, only the parties to a specific transaction and CFIUS know (1) if a transaction has been subject to review by CFIUS and (2) whether CFIUS required mitigation.[10] Team Telecom's risk assessments are generally not made public either. The most the public may learn in a relevant Commission proceeding is what mitigation measures Team Telecom re-

(2019) ("*Supply Chain Order*"); *see* Comments of Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc., WC Docket No. 18-89, at 3 (filed Aug. 31, 2020) ("Huawei Comments") (arguing that the Secure Networks Act does not "ratify" the *Supply Chain Order*, and that the Secure Networks Act confirms that the Commission lacks authority to make designations under that *Order*).

7 NCTA Comments at 5.

8 USTelecom Comments at 3.

9 *See* NCTA Comments at 10.

10 *See* 31 C.F.R. § 800.802 (regarding confidentiality in the CFIUS process).

quired after reviewing a transaction for foreign investment. As Huawei explained in its prior comments, relying on non-public determinations raises substantial due process concerns for regulated parties against whom such information will be used in a critical way.[11]

In addition, relying on CFIUS or Team Telecom determinations is unnecessary given the involvement of the agencies that comprise CFIUS and Team Telecom in other relevant bodies identified in the Secure Networks Act.[12] For example, CFIUS is chaired by the Department of Treasury and includes as members the Departments of Justice, Homeland Security, Commerce, Defense, State, and Energy, and the Offices of the U.S. Trade Representative and of Science & Technology Policy.[13] By comparison, the Federal Acquisition Security Council named in Section 2(c)(1) of the Secure Networks Act as an example of an "executive branch interagency body with appropriate national security expertise" already includes the Departments of Homeland Security, Justice, Defense, and Commerce, as well as the Office of Management and Budget, the Office of the Director of National Intelligence, the General Services Administration, and "such other executive agencies as determined by the Chairperson of the Council."[14] There also is significant overlap between CFIUS and Team Telecom, with Team Telecom including as members the Secretary of Defense, Attorney General, Secretary of Homeland Security, and "the head of any other exec-

---

11 *See* Huawei Comments at 8, 19-20.

12 *See* NCTA Comments at 10.

13 Dep't of Treasury, CFIUS Overview, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview. The White House's Office of Management and Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council observe and sometimes participate in CFIUS. The Director of National Intelligence and Secretary of Labor are non-voting, *ex officio* members of CFIUS. *See also* 50 U.S.C. § 4565.

14 41 U.S.C. § 1322(b)(1).

utive department or agency, or any Assistant to the President, as the President determines appropriate."[15] Moreover, as CTIA notes, CFIUS and Team Telecom "proceedings tend to focus on operational and governance issues related to foreign investment." CFIUS and Team Telecom "are not structured to make determinations of general supply chain risk," so "[t]heir work … may not help inform Commission determinations about the risk posed by particular equipment or services."[16] The Secure Networks Act already provides the Commission a plethora of national security agencies upon whose determinations the Commission must rely to develop the Covered List without relying on CFIUS or Team Telecom.

II. THE COMMISSION CAN ADD EQUIPMENT AND SERVICES TO THE COVERED LIST ONLY IF THAT EQUIPMENT OR THOSE SERVICES ARE PRESENTLY CAPABLE OF MEETING THE REQUIREMENTS PRESCRIBED IN SECTION 2(B)(2) OF THE SECURE NETWORKS ACT.

As Huawei previously explained, the Secure Networks Act plainly does not make ineligible for universal service funding *all* equipment from entities that are subject to specific national security determinations by Congress or other agencies under Sections 2(b)(1) and (c).[17] Rather, Congress in the Secure Networks Act bars use of subsidy funds to purchase or maintain equipment and services "if and only if" the equipment or services fall within statutorily prescribed categories in Sections 2(b)(1) *and* 2(b)(2).[18]

Indeed, most commenting parties agree that equipment and services can be included on the Covered List only if such equipment or services also meet the criteria prescribed in Section

---

15 Exec. Order. No. 13913, 85 Fed. Reg. 19643 (Apr. 8, 2020), https://www.govinfo.gov/content/pkg/FR-2020-04-08/pdf/2020-07530.pdf.

16 Comments of CTIA – The Wireless Association, WC Docket No. 18-89, at 14 (filed Aug. 31, 2020) ("CTIA Comments").

17 Huawei Comments at 4-5.

18 Huawei Comments at 3-4 (citing Secure Networks Act, § 2(b)).

2(b)(2).[19] NCTA recognizes that Congress envisioned that the Commission would place on the Covered List only equipment and services from providers identified by the agencies enumerated in the Secure Networks Act and only when such equipment and services also meet the specific characteristics outlined in Section 2(b)(2).[20] If the Commission could rely solely on external determinations to satisfy both Sections 2(b) and (c), without evaluating equipment for technical issues under Section 2(b)(2), then the entirety of Section 2(b)(2) would be superfluous.[21]

Commenters also agree that, to the extent equipment is identified under Section 2(b)(2) in reliance on the 2019 NDAA, that equipment should be required to have routing, redirecting, or visibility capabilities because the NDAA relies on those capabilities to identify equipment presenting national security risks. Specifically, Congress exempted equipment without those capabilities from the prohibitions imposed by Section 889 of the 2019 NDAA. As CTIA notes, a broad construction of Section 2(b) of the Secure Networks Act would be inconsistent with the risk-based approach taken in Section 889 that resulted in excluding only equipment or services that "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles."[22] Thus, as NCTA has explained, where Section 889 serves

---

[19] *See* CCA Comments at 3-4 (explaining that Section 2 of the secure Networks Act "describes how the Commission must construct" the Covered List); CTIA Comments at 9-10 (urging the Commission to construe "covered equipment and services" narrowly to avoid an "unduly broad" construction that "goes beyond the text of Section 2(b)(2)"); Huawei Comments at 3-4; NCTA Comments at 5-6 (noting that the statute authorized the Commission to place equipment or services on the Covered List "only if such equipment or service is capable of (i) routing or redirecting traffic, (ii) remotely disrupting networks, or (iii) posing an unacceptable risk to national security and the safety of U.S. persons"); USTelecom Comments at 3 (arguing that "when a federal agency or entity identifies broader classes or categories equipment the Commission must apply the section 2(b)(2) criteria to determine whether equipment is 'covered equipment'").

[20] NCTA Comments at 5-6.

[21] *See Yates* v. *United States*, 135 S. Ct. 1074, 1085 (2015) (rejecting a statutory interpretation that would "render superfluous an entire provision passed in proximity as part of the same Act").

[22] CTIA Comments at 10.

as the basis for including equipment on the Covered List, the Commission must "ensure fidelity to the specific limits in that statute" with the range of equipment on the Covered List being "coterminous" with the restrictions in Section 889.[23]

III. THE COMMISSION MUST PROVIDE NOTICE BEFORE ADDING EQUIPMENT OR SERVICES TO THE COVERED LIST.

There also is broad agreement among commenting parties that the Commission must provide public notice before adding equipment and services to the Covered List. Equipment vendors and carriers alike need sufficient notice of the Commission's intent to add equipment or services to the list to allow time for vendors and carriers to assess the potential impacts of the Covered List and make necessary network modifications.

Any process the Commission adopts to add equipment or services to the Covered List should be open and transparent, and should not rely on informal determinations or determinations that have not been made public.[24] As the Rural Wireless Association ("RWA") notes, an agency's determination that equipment or services pose a national security threat is inadequate; providers should be specifically informed that certain equipment or services will be placed on the Covered List.[25] Moreover, the Commission would benefit from providing notice and an opportunity for comment so that stakeholders can inform the Commission of the potential impacts of updates to the Covered List or seek clarification regarding models of equipment or components to be included

---

[23] NCTA Comments at 6.

[24] CTIA Comments at 15-17 (advocating for transparency and notice during implementation of the Secure Networks Act).

[25] Comments of Rural Wireless Association, WC Docket No. 18-89, at 2 (filed Aug. 31, 2020) ("RWA Comments").

on the Covered List.[26] And, as Huawei has explained, failure to provide prior notice would violate due process rights for entities who may not have had any prior knowledge of or opportunity to challenge the relevant specific national security determination(s) upon which the Commission intends to rely to place equipment on the Covered List.[27]

The Commission also should provide notice of which specific equipment and services it proposes to designate as covered, and seek comment on proposals to add specific equipment and services to the Covered List. Huawei agrees with RWA that when an agency's determination names only an entity, the Commission should issue—and seek comment on—a proposal detailing which of the entity's specific equipment and services it believes should be covered.[28] The Commission should be as transparent and specific as possible to ensure that providers are not left to guess which models or version of equipment or services are sufficient to make something "capable" of posing an unacceptable risk.[29] And, as NTCA urges, the Commission should issue an order containing an initial designation identifying all equipment or services posing a threat to national security *before* a ban becomes effective.[30]

Under no circumstances should the Commission engage in a confidential process in developing the Covered List, as one commenter suggests.[31] Using a confidential process in which participation is limited to "trusted domestic technology companies" would deprive key stakeholders—including carriers most likely to use covered equipment or services and understand the capabilities

---

[26] *See* NCTA Comments at 11-12 (urging the FCC to provide notice and an interim transition period prior to placement of new equipment or services on the Covered List).

[27] *See* Huawei Comments at 19-20.

[28] RWA Comments at 2.

[29] *See* NCTA Comments at 11.

[30] Comments of NTCA – The Rural Broadband Association, WC Docket No. 18-89, at 2-4 (filed Aug. 31, 2020).

[31] *See* Comments of Dell Technologies, Inc., WC Docket No. 18-89, at 1-2 (filed Aug. 31, 2020).

of specific equipment in question—the opportunity to provide meaningful input as the Commission considers adding equipment and services to the Covered List.

IV. CONCLUSION

For the foregoing reasons and those stated in Huawei's earlier submissions, the Commission's discretion in implementing the Secure Networks Act is limited in key ways, and any rules the Commission adopts must comply with the plain text of the Act.

Respectfully submitted,

/s/ Andrew D. Lipman

Glen D. Nager
Michael A. Carvin
Shay Dvoretzky

JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
macarvin@jonesday.com
sdvoretzky@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

September 14, 2020